NWU®

ITRI 625

Pfleeger Chapter 9

Privacy concepts

- Privacy is the right to control who knows certain aspects about you, your communications, and your activities.

- Information privacy has three aspects, sensitive data, affected parties, and controlled disclosure.

1. Controlled disclosure. As soon as you give out your number for example, your control is diminished because it depends in part on what someone else does. You do not control the other person.

2. Sensitive data. Some examples of data many people consider private include, identity, finances, legal matters, religion, etc.

3. Affected subject. The entity involved governs the data and possible consequences.

Computer related privacy problems

- The eight dimensions of computer related privacy are:

1. Information collection. Only with knowledge and explicit consent.
2. Information usage. Only for certain specified purposes.
3. Information retention. Only for a set period of time.
4. Information disclosure. Only to authorized people.
5. Information security. Appropriate mechanisms are used to ensure protection.
6. Access control. All modes of access are controlled.
7. Monitoring. Logs are maintained showing all accesses.
8. Policy changes. Less restrictive policies are never applied after-the-fact to already obtained data.

Steps to protect against privacy loss

- Several steps that any entity can take to help safeguard private data include:

- Data minimization.
- Data anonymization.
- Audit trail.
- Security and controlled access.
- Training.
- Quality.
- Restricted usage.
- Data left in place.
- Policy.

Authentication and privacy

- Authentication can refer to authenticating an individual, identity, or attribute.
- An individual is an unique person. There are relatively few ways of identifying an individual, and usually weak authentication is acceptable.
- An identity is a character string or similar descriptor. From a privacy standpoint, there may or may not be ways to connect different identities. Depending on the application, it can typically be done through linking, especially when authentication is not ideal and anonymity is required.
- An attribute is a characteristic. By linking various characteristics, privacy can quite often be jeopardized. Research has indicated that the process of effectively anonymizing data is extremely difficult.

Privacy on the web

- The internet is perhaps the greatest threat to privacy.
- It is like a nightmare of a big, unregulated bazaar, where every word you speak can be heard by many others.
- Payments on the web are perhaps one of the main privacy concerns, and nowadays mainly credit cards or payment schemes are used for online transactions.
- Sites and portals often require registering before being able to use their services. More often than not this information is used for marketing or to show that advertisements are warranted.
- Third party ads, contests and offers are great ways for companies to collect information and draw links.

Privacy on the web *cont.*

- Precautions for web surfing include limiting cookies and web bugs, two technologies that are frequently used to monitor a user's activities without the user's knowledge.

- Cookies are files of data sent by a website, and are a cheap way of transferring storage needs from a website to a user.

- Third party cookies are for organizations other than the webpage's owner.

- A cookie is a tracking device, whereas a web bug is an invisible image that invites or invokes a process. The image is typically 1 x 1 pixel, so virtually invisible on modern resolutions.

Privacy on the web *cont.*

- Spyware code is designed to spy on a user to obtain information.
- Keystroke loggers, the computer equivalent of a telephone wiretap.
- Hijackers, software that hijacks a program installed for a different purpose.
- Adware, displays selected ads in pop-up windows with the aim of obtaining personal information.
- Drive-by installation, a means of tricking a user into installing software. It conceals from the user the real code being installed.

Impacts on emerging technologies

- Applications of three emerging technologies have inherent risks for privacy.

1. Radio frequency identification (RFID). Small, low power wireless radio transmitters. When a tag receives a signal it sends its ID number in response. Its major concerns are the ability to track people wherever, and correctness.

2. Electronic voting. Ensuring anonymity whilst voting using computers is extremely difficult. Both in capturing the vote and in transmitting it to the election headquarters.

3. Voice over IP (VoIP). Even if solidly encrypted, the source and destination of the phone call will be somewhat exposed through packet headers.

4. Internet of Things (IoT). Insecure products can lead to potentially catastrophic consequences.

Questions

- Any Questions?